(FY 09) PIA: System Identification

Program or System Name:	REGION 5> VBA> Philadelphia ITC> LAN
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-02-00-01-1120-00
Description of System / Application / Program:	The Philadelphia ITC is responsible for the implementation, o systems that assist VA Regional Offices (ROs), the Insurance C and medical care to the nation's Veterans and their families. technology services to the VBA nationwide for the Veterans I applications. The Philadelphia ITC operates the Information T help desk, and provides information technology problem reso additional information regarding the LAN.)

Facility Name:	Philadelphia Information Technology Center (PITC)

Title:	Name:	Phone:
Privacy Officer:	Kenneth Young	215-842-2000 ext. 4503
Information Security Officer:	James Boring	215-842-2000 ext. 4613
Chief Information Officer	Carol Winter	215-381-3030
Person Completing Document:	Stephen M. King	202-461-9454
System Owner:	Kevin C. Causley	202-461-9170
Alternate Information Security Officer	Charles McCarron	215-842-2000 ext. 4203
Facility Chief Information Officer	Mary D. Barley	202-461-9175
Other Titles:		
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	06/2008	
Date Approval To Operate Expires:	08/15/2011	

What specific legal authorities authorize this program or system:	VA Directives 6051, 6102, 6301, 6320, and 6500.
What is the expected number of individuals that will have their PII stored in this system:	None
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	14 years
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Date of Report (MM/YYYY):	04/2009

If answers 'Yes' to one or more of the following, please check the appropriate box, continue to the next tab, a
form. If none have been checked then skip to Signatures tab, obtain the appropriate signatures, and submit

- ☐ Has a PIA NOT been completed within the last three years?
- ☐ Have any changes been made to the system since the last PIA?
- ☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☐ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☐ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☐ Does this system/application/program collect, store or disseminate the SSN?

›peration and maintenance of information
Center, and Medical Centers in providing benefits
The Philadelphia ITC provides information
nsurance, Email, Intranet, and Internet
Technology Support Center (ITSC), which is VBA's
olution to all VBA organizations. (See Tab 8 for

Email:

ken.young@va.gov
james.boring@va.gov
carol.a.winter@va.gov
stephen.king3@va.gov
kevin.causley@va.gov
charles.mccarron@va.gov
mary.barley@va.gov

and complete the remaining questions on this
this document.

:tors, or others performing work for t
nique identifier, symbol, or oth

(FY 09) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?	No
if the answer above is no, please skip to row 16.	
For each applicable System(s) of Records, list: 1. All System of Record Identifier(s) (number): 2. Name of the System of Records: 3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	
Does the System of Records Notice require modification or updating?	
	(Please Select Yes/No)
Is PII collected by paper methods?	No
Is PII collected by verbal methods?	No
Is PII collected by automated methods?	No
Is a Privacy notice provided?	
Proximity and Timing: Is the privacy notice provided at the time of data collection?	
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	

(FY 09) PIA: Notice

Please fill in each column for the data types selected.

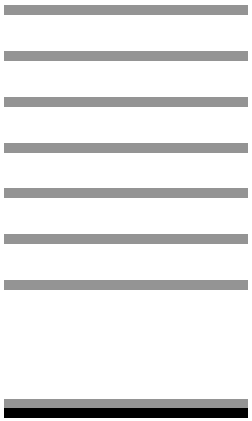
Data Type	Collection Method	What will the subjects be told about the information collection?	How is this messaged conveyed to them?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)			
Family Relation (spouse, children, parents, grandparents, etc)			
Service Information			
Medical Information			
Criminal Record Information			
Guardian Information			
Education Information			
Benefit Information			
Other (Explain)			

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	No		

Family Relation (spouse, children, parents, grandparents, etc)	No	
Service Information	No	
Medical Information	No	
Criminal Record Information	No	
Guardian Information	No	
Education Information	No	
Benefit Information	No	
Other (Explain)		
Other (Explain)		
Other (Explain)		

How is a privacy notice provided?

Additional Comments



(FY 09) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization					
Other Veteran Organization					
Other Federal Government Agency					
State Government Agency					
Local Government Agency					
Research Entity					
Other Project / System					
Other Project / System					
Other Project / System					

(FY09) PIA: Access to Records

Does the system gather information from another system? Please enter the name of the system:	No
Does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	☐ Through a Written Request ☐ Submitted in Person ☐ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY09) PIA: Secondary Use

Will PII data be included with any secondary use request?	
if yes, please check all that apply:	☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)
Describe process for authorizing access to this data. Answer:	

(FY 09) PIA: Program Level Questions

Does this PIA contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer:

How is data checked for completeness?

Answer:

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer:

How is new data verified for relevance, authenticity and accuracy?

Answer:

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 09) PIA: Retention & Disposal

What is the data retention period?

Answer:

Explain why the information is needed for the indicated retention period?

Answer:

What are the procedures for eliminating data at the end of the retention period?

Answer:

Where are these procedures documented?

Answer:

How are data retention procedures enforced?

Answer:

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 09) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 09) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	No
Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	No

If 'No' to any of the 3 questions above, please describe why:

Answer: On an annual basis, the VA Chief Information Officer (CIO), in conjunction with system owners and information owners, and with advice from the VA Office of Inspector General (OIG), evaluate the Department's overall IT security posture. This evaluation includes identification of significant security performance gaps, the prioritization of key POA&M weakness areas for immediate remediation action, as well as the designation of certain security areas that would benefit from enterprise-wide management of a single security solution, thereby effectively targeting those areas for action that would most improve the Department's security posture in the near-term.	
Is adequate physical security in place to protect against unauthorized access? If 'No' please describe why: Answer:	Yes
Explain how the project meets IT security requirements and procedures required by federal law.	

Answer: A standardized Department methodology based on the direction in National Institute of Standards and Technology (NIST) guidance is used to continuously monitor, test and evaluate security for this major application. The approximately 60 common security controls provided by the Office of Information and Technology (OIT), or other respective VA Program Office, are tested every year. Application-specific security testing evaluates approximately one-third of the remaining 90 controls on an annual basis, with the entire respective application NIST Special Publication (SP) 800-53 security control baseline—at the Federal Information Processing Standard (FIPS) 199 level of moderate--being tested over each three-year period. The testing supports certification and re-accreditation requirements, as well as Federal Information Security Management Act (FISMA) requirements to annually test the operational, management, and technical controls of each Department system. The specific controls identified for testing are selected by OIT Operations, with advice from the VA Office of Cyber Security (OCS), and include ke

---

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- ☑ Air Conditioning Failure
- ☑ Chemical/Biological Contamination
- ☑ Blackmail
- ☑ Bomb Threats
- ☑ Cold/Frost/Snow
- ☑ Communications Loss
- ☑ Computer Intrusion
- ☑ Data Destruction
- ☑ Data Disclosure
- ☑ Hardware Failure
- ☑ Malicious Code
- ☑ Computer Misuse
- ☑ Power Loss
- ☑ Sabotage/Terrorism
- ☑ Storms/Hurricanes
- ☑ Substance Abuse
- ☑ Theft of Assets
- ☑ Theft of Data

- [x] Data Disclosure
- [x] Data Integrity Loss
- [x] Denial of Service Attacks
- [x] Earthquakes
- [x] Eavesdropping/Interception
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [x] Theft of Data
- [x] Vandalism/Rioting
- [x] Errors (Configuration and Data Entry)
- [x] Burglary/Break In/Robbery
- [x] Identity Theft
- [x] Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- [x] Risk Management
- [x] Access Control
- [x] Awareness and Training
- [x] Contingency Planning
- [x] Physical and Environmental Protection
- [x] Personnel Security
- [x] Certification and Accreditation Security Assessments
- [x] Audit and Accountability
- [x] Configuration Management
- [x] Identification and Authentication
- [x] Incident Response
- [x] Media Protection

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer:

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?
(Choose One)

- ☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☑ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?
(Choose One)

- ☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☑ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?
(Choose One)

- ☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☑ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

Please add additional controls:

FY 09: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on. Please indicate the question you are responding to and then add your comments.

Major applications that are hosted on servers that are physically part of the PITC LAN are certified and accredited as separate systems, and PIAs have been separately developed for each of those major applications. The three minor applications listed below do not process or store PII data as a routine course of operation, although each minor application could communicate PII data if the user included PII in the message content. In such cases, the methods of securing the PII data has been addressed in the relevant SSP for the major application that will process and store that data. It is the responsibility of the user to ensure that PII is appropriately protected when transmitting the data via BlackBerry Messenger, Enterprise email tools, or facsimile equipment.

Philadelphia ITC LAN Applications

Enterprise Wireless Messaging System (BlackBerry)
The BlackBerry Messenger system provides IMAP server backbone support for OI&T and all VBA wireless cell phone messaging conducted between authorized users. The IMAP server creates a temporary file with connection information for you and your contacts. The server determines which contacts are logged on and sends that information to your BlackBerry, as well as letting the contacts know that you're available. After that, the server functions as a typical mail server.

VBA Enterprise Messaging System
The MS Exchange architecture is comprised of 11 Exchange mailbox servers running Microsoft Cluster Service (MCS) located at the Philadelphia ITC and 1 stand alone Exchange mailbox server located in Manila. Two Outlook Web Access (OWA) servers provide remote mailbox access. Four bridgehead servers route mail to external sites and Internet users. Database storage is provided by two Storage Access Networks. The server operating system is Windows Enterprise 2003. Exchange software consists of MS Exchange 2003 SP2.

LGY Centralized Fax System
The centralized fax system (RightFax) supports the Loan Guaranty Electronic Lender Folder (ELF) program. The RightFax architecture is comprised of comprised of (4) Compaq servers in a cluster configuration. The operating system is Microsoft Windows 2000. The application software is Captaris v8.7. The current telephone system in use to provide access to RightFax is (2) T1 lines.

(FY 09) PIA: Final Signatures

Facility Name: Philadelphia Information Technology Center (PITC)

Title:	Name:	Phone:	Email:
Privacy Officer:	Kenneth Young	215-842-2000 ext. 4503	ken.young@va.gov
KENNETH E YOUNG Digitally signed by KENNETH E YOUNG DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)96, cn=KENNETH E YOUNG, email=ken.young@va.gov Date: 2009.05.11 08:28:30 -04'00'			
Information Security Officer:	James Boring	215-842-2000 ext. 4613	james.boring@va.gov
JAMES BORING Digitally signed by JAMES BORING DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS Incorp. by Ref., LIAB.LTD(c)96, cn=JAMES BORING, email=james.boring@va.gov Date: 2009.05.11 08:37:18 -04'00'			
Chief Information Officer:	Carol Winter	215-381-3030	carol.a.winter@va.gov
CAROL A WINTER Digitally signed by CAROL A WINTER DN: o=Department of Veterans Affairs, ou=Dept. of Veterans Affairs, Internal Staff, ou=www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)96, cn=CAROL A WINTER, email=carol.a.winter@va.gov Date: 2009.05.12 11:53:29 -04'00'			
Person Completing Document:	Stephen M. King	202-461-9454	stephen.king3@va.gov
Signature not verified! STEPHEN M. KING Digitally signed by: STEPHEN M. KING DN: CN = STEPHEN M. KING O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2009.05.13 13:01:29 -05'00' Reason: I am the author of this document			
System / Application / Program Manager:	Kevin C. Causley	202-461-9170	kevin.causley@va.gov
Signature not verified! BARLEY, MARY, VBAVACO Digitally signed by: BARLEY, MARY, VBAVACO DN: CN = BARLEY, MARY, VBAVACO O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2009.05.15 11:29:43 -05'00' Reason: I am approving this document			

Date of Report:	04/01/2009
OMB Unique Project Identifier	029-00-02-00-01-1120-00
Project Name	REGION 5> VBA> Philadelphia ITC> LAN